(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 422 875 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.05.2004 Bulletin 2004/22

(51) Int Cl.[7]: **H04L 12/28**

(21) Application number: **03025633.3**

(22) Date of filing: **06.11.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **08.11.2002 US 290650**

(71) Applicant: **DoCoMo Communications Laboratories USA, Inc.**
San Jose, CA 95110 (US)

(72) Inventors:
- **Wu, Gang**
  San Jose, CA 95110 (US)
- **Watanabe, Fujio**
  San Jose, CA 95110 (US)
- **Hagen, Alexander**
  San Jose, CA 95110 (US)

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Wireless network handoff key

(57) A handoff key is provided for facilitating a handoff of a wireless terminal (12) from a first access point to a second access point. The handoff key may be generated by a server and communicated to the first and second access points. Alternatively, the handoff key may be generated one of the access points and transmitted to the other access point. The first access point may transmit the handoff key to the wireless terminal before the handoff. Shortly after the handoff, the wireless terminal and the second access point may communicate data encrypted with the handoff key. Later, an authentication server (36) may authenticate the wireless terminal, causing the second access point to provide the wireless terminal (12) with a session key. Thereafter, the wireless terminal (12) and the second access point may communicate data encrypted with the session key.

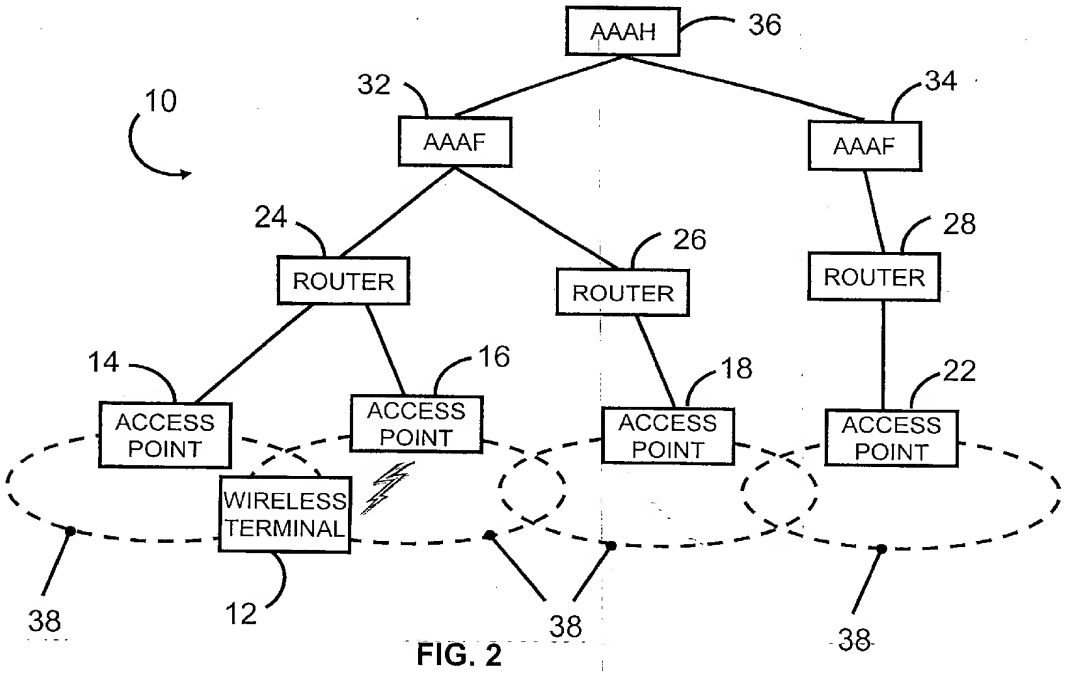


FIG. 2

EP 1 422 875 A2

Description

Field of the Invention

[0001] The present invention relates generally to a wireless network environment, and more particularly to a method and system for providing a handoff key for a wireless network environment.

Background of the Invention

[0002] One common distributed computing environment is a local area network (LAN). A LAN is a peer-to-peer communication network that enables terminals or stations to communicate directly on a point-to-point or point-to-multipoint basis. A LAN is optimized for a moderate-sized geographic area, such as a single office building, a warehouse, or a campus. In most LANs, communications are transmitted via wires.

[0003] Recently, wireless LAN (WLAN) technology has become popular. A WLAN operates in much the same manner as a wired LAN, except the transmission medium is radio waves rather than wires. In a typical WLAN topography, terminals communicate with a larger network, such as a wired LAN or wide area network (WAN), through access points. An access point is a terminal that acts as a gateway between the WLAN and the larger network.

[0004] In wired LANs, physical security can be used to prevent unauthorized access. However, physical security may be impractical in WLANs, so an authentication process for network access and an encryption/decryption mechanism may be required for security. Access points of a WLAN may illustratively be located in meeting rooms, restaurants, hallways, corridors, lobbies, and the like. A terminal accessing the WLAN may move out of range of a first access point and into range of a second access point. When this occurs, a handover (handoff) from the first access point to the second access point may be required.

[0005] Generally, the terminal must communicate terminal authentication packets with an authentication server, which may be a home registration server, before it may access the WLAN through the second access point. This authentication process could be time consuming, interrupting communications between the terminal and another terminal. This interruption could be problematic, especially for real-time applications, such as streaming applications and voice over IP (VoIP) applications, which require uninterrupted communications for smooth operation and quality of service (QoS) gaurentees. It would be desirable to provide method and system for quickly authenticating a terminal during a handoff.

Summary of the Invention

[0006] A method for handover in a wireless communication network is provided. A handoff WEP key may be provided to a first and a second access point. The first access point may transmit the handoff WEP key to a wireless terminal associated therewith. The second access point may authenticate the wireless terminal, and communicate data packets encrypted with the handoff WEP with the wireless terminal.

[0007] The first access point may only transmit the handoff WEP key to the wireless terminal if the wireless terminal is actively communicating via the first access point. The first access point may encrypt the handoff WEP key with a session WEP before transmitting it to the wireless terminal. The second access point may authenticate the wireless terminal with an authentication server. Authenticating the wireless terminal may include communicating authentication packets via the second access point between the wireless terminal and the authentication server. Authenticating the wireless terminal may also include transmitting terminal authorization packets from the authentication server to the second access point.

[0008] The terminal authentication packets may be transmitted from the wireless terminal to the second access point encrypted by the handoff WEP key. Alternatively, the terminal authentication packets may be transmitted from the wireless terminal to the second access point unencrypted. After the wireless terminal is authenticated by the authentication server, the second access point may transmit a session WEP key to the wireless terminal after.

[0009] A server may generate the handoff WEP key, and transmit it from the server to the first and second access points. The second access point may authenticate the wireless terminal by sending a challenge message encrypted with the handoff WEP key to the wireless terminal, receiving the decrypted challenge message from the wireless terminal, and determining if the wireless terminal correctly decrypts the challenge message.

[0010] Additionally, a wireless network is provided. The wireless network may include a wireless terminal that may receive and encrypt data with a handoff WEP key. The wireless terminal may transmit the encrypted data. The wireless network may also include a first access point that may transmit the handoff WEP key to the wireless terminal, and a second access point that may receive encrypted data from the wireless terminal and decrypt it with the handoff WEP key.

[0011] The wireless network may further include a server coupled to the first and second access points that generates the handoff WEP key and transmits it to the first and second access points. The wireless network may also include a

server coupled to the first and second access points that authenticates the wireless terminal.

[0012] Additionally, a wireless access point having a memory is provided. The memory may include instructions to receive a packet and delete the packet if the packet is a data packet that is not encrypted with a handoff WEP key. The memory may include instructions to decrypt and transmit the packet if the packet is a data packet that is encrypted with a handoff WEP key. The memory may also include instructions to transmit the packet if the packet is a terminal authentication packet.

[0013] Further, the memory may include instructions to read the media access control address for a terminal that sent the packet and determine whether the memory includes a session WEP key for the terminal. If so, the memory may include instructions to decrypt and transmit the packet.

[0014] Additionally, a wireless terminal having a memory is provided. The memory may include a code segment that receives and decrypts a handoff WEP key that has been encrypted with a first session WEP key. The memory may also include a code segment that encrypts data with the handoff WEP key and a code segment that transmits the encrypted data. Further more, the memory may include a code segment that receives and decrypts a second session WEP key that is encrypted with the handoff WEP key.

[0015] The memory may also include a code segment that that encrypts and decrypts data with the first session WEP key until the handoff WEP key is received, a code segment that encrypts and decrypts data with the handoff WEP key until the second session WEP key is received, and a code segment that encrypts and decrypts data with the second session WEP key after the second session WEP is received.

[0016] Additionally, a wireless network is provided. The wireless network may include a means for providing a handoff WEP key to first and second access points. The wireless network may also include means for transmitting the handoff WEP key from the first access point to a wireless terminal. Also, the wireless network may include means for authenticating the wireless terminal with the second access point, and means for communicating data packets encrypted with the handoff WEP key between the second access point and the wireless terminal. Furthermore, wireless network may include means for encrypting the handoff WEP key with a session WEP key before transmitting it to the wireless terminal.

Brief Description of the Drawings

[0017] FIG. 1 is a system-level block diagram of a distributed computing system.

[0018] FIG. 2 is a block diagram of a sub-network including a wireless segment.

[0019] FIG. 3 is a packet communication diagram for a shared key handoff procedure.

[0020] FIG. 4 is a packet communication diagram for an open system handoff procedure.

[0021] FIG. 5 is a flow chart for a parallel processing security procedure.

[0022] FIG. 6 is a flow chart for a serial processing security procedure.

Detailed Description of the Presently Preferred Embodiments

[0023] FIG. 1 is a system level block diagram of a distributed computing system 2. The distributed computing system 2 may be any computing environment where one or more terminals communicate with one or more other terminals. The configuration of the distributed computing system 2 shown in FIG. 1 is merely illustrative. The distributed computing system 2 includes: a wireless terminal 12, a network 8, and a terminal 6. The wireless terminal 12 may communicate with the terminal 6 via the network 8. The network 8 may be a global network, such as the Internet, a wide area networks (WAN), or a local area network (LAN). The network 8 may include wireless communication networks, local area networks (LAN), wide area networks (WAN), satellite networks, Bluetooth networks, or other types of networks. The network 8 preferentially may include a sub-network 10. An illustrative sub-network 10 is shown in FIG. 2.

[0024] The terminal 6 and the wireless terminal 12 may each be a desktop computer, a server, a laptop computer, a personal digital assistant (PDA), a pocket PC, a wireless telephone, or some other communications enabled device. The terminals 6 and 12 may each be configured as a client, as a server, or as a peer for peer-to-peer communications. Peer-to-peer communications may include voice over IP (VoIP), video teleconferencing, text messaging, file sharing, video streaming, audio streaming, or other direct communications. The terminals 6 and 12 may be capable of wireless communications, and may be coupled to the network 8 directly or through an access point. The terminal 6 and the wireless terminal 12 may each have a memory including instructions for operation.

[0025] FIG. 2 is a block diagram of an illustrative sub network 10 of the network 8. The sub-network 10 may include an authentication, authorization, and accounting home (AAAH) server 36; authentication, authorization, and accounting foreign (AAAF) servers 32 and 34; access routers 24, 26, and 28; and access points 14, 16, 18, and 22. Even though elements of the sub-network 10 are shown as directly coupled in FIG. 2, the elements may be indirectly coupled and separated geographically. The simplified coupling is shown in order to more clearly illustrate communication paths.

[0026] The AAAH server 36 may authenticate a set of terminals. This set of terminals may be associated with the AAAH server 36. The AAAH server 36 may have a memory including codes segments and instructions for operation.

The AAAH server 36 may include an authentication server that maintains information regarding the identification, authorization, and billing of the associated terminals. The credentials or the identities of the associated terminals may be verified by the AAAH server 36. Also, whether the associated terminals are authorized to access a resource, such as a network, may be determined by the AAAH server 36.

[0027] A terminal authentication procedure may be used by the AAAH server 36. The terminal authentication procedure may use digital certificates, username and password pairs, and other challenge and response protocols that facilitate authenticating the associated terminals. As part of the terminal authentication procedure, the AAAH server 36 may communicate terminal authentication packets with the associated terminals and terminal authorization packets with authenticators. The terminal authentication packets may contain digital certificates, keys, usernames, passwords, challenge text, challenge messages, and the like to facilitate verifying the identity or credentials of the terminal. Terminal authorization packets may indicate that an associated terminal is authorized for a level of access to a resource, such as a network. The level of access may indicate full access, no access, or limited access.

[0028] The terminal authentication procedure may comply with the Remote Authentication Dial-In User Service (RADIUS) protocol specified in Internet Engineering Task Force (IETF) Request for Comments (RFCs) 2865 and 2866. The terminal authentication procedure also may comply with an authentication process specified in the IEEE 802.1x standard.

[0029] After authorizing an associated terminal, the AAAH server 36 may track (account for) resources utilized by the associated terminal. For example, the AAAH server 36 may track metrics regarding access of a network by the associated terminal. Information regarding resource utilization by an associated terminal may be provided to the AAAH server 36.

[0030] The AAAH server 36 may generate an encryption key. The encryption key may be a handoff key. The handoff key may be wired equivalent privacy (WEP) key. The term "handoff WEP key" is used herein for an encryption key that may be used simultaneously by more than one access point for encrypted communications with one or more wireless terminals.

[0031] The AAAH server 36 may provide handoff WEP keys to access points. During a handoff of a terminal from a first access point to a second access point, communications between the terminal and the second access point may be encrypted by a handoff WEP key. The AAAH server 36 may generate and provide new handoff WEP keys with a frequency adequate for reasonably secure communications.

[0032] The AAAF servers 32 and 34 may also authenticate sets of terminals. The AAAF servers 32 and 34, however, may be associated with different sets of terminals than the set associated with the AAAH server 36. For terminals associated with the AAAH server 36, the AAAH server 36 is the "home server", and the AAAF servers 32 and 34 are "foreign servers".

[0033] For terminals associated with the AAAF server 32, the AAAF server 32 is the "home server" and the AAAH server 36 is the "foreign server". For clarity, the names of the servers have been chosen according to their relationship with the illustrative wireless terminal 12. Foreign servers are discussed to illustrate the versatility of the present invention, not to limit it.

[0034] The AAAF servers 32 and 34 may indirectly authenticate terminals associated with the AAAH server 36. The AAAF servers 32 and 34 may each have a memory including code segments and instructions for operation. The AAAF servers 32 and 34 may have no innate information regarding the identities of terminals associated with the AAAH server 36. Nevertheless, the AAAF servers 32 and 34 may indirectly authenticate and authorize terminals associated with the AAAH server 36 by communicating terminal authentication packets and terminal authorization packets with the AAAH server 36. The AAAF servers 32 and 34 may account for resources utilized by terminals associated with the AAAH server 36, and provide accounting information to the AAAH server 36.

[0035] Each AAAF server 32 and 34 may generate handoff WEP keys. Each AAAF server 32 and 34 may generate handoff WEP keys for access points associated therewith. Alternatively, the AAAF server 32 and 34 may receive a common handoff WEP key from the AAAH server 36.

[0036] The access routers 24, 26, and 28 may route packets. Each access router 24, 26, and 28 may be capable of determining a next network node to which a received packet should be forwarded. A network node may be a terminal, a gateway, a bridge, or another router. Each access router 24, 26, and 28 may be coupled to other sub-networks (not shown) and provided a route for packets between the sub-network 10 and the other sub-networks.

[0037] Each access point 14, 16, 18, and 22 may provide access to a network. A memory including code segments and instructions for operation may be included in each access point 14, 16, 18, and 22. Access points 14, 16, 18, and 22 may be edge points of a network. Each access point 14, 16, 18, and 22 may be an authenticator, and may require a terminal to be authenticated by an authentication server in order for the terminal to access the network. Before a terminal has been authenticated by an authentication server, the access points 14, 16, 18, and 22 may only allow the terminal to communicate terminal authentication packets with an authentication server. After the terminal has been authenticated by an authentication server, the access points 14, 16, 18, and 22 may allow the terminal to communicate data packets via the network.

[0038] The access points 14, 16, 18, and 22 may each include a wireless access port having an associated spatial coverage area 38. The coverage area 38 of each access point 14, 16, 18, and 22 may overlap with the coverage area 38 of one or more adjacent access points 14, 16, 18, and 22. Wireless terminals within the coverage area 38 of an access point 14, 16, 18, or 22, may associate with and communicate with the respective access point.

[0039] Encryption keys may be provided by access points 14, 16, 18, and 22 to wireless terminals within the coverage area 38 of the respective access point 14, 16, 18, and 22. Each encryption key may be a session key. A session key may be wired equivalent privacy (WEP) key. The term "session WEP key" is used herein for an encryption key that may be used for encrypted communications between an access point and a wireless terminal. Access points 14, 16, 18, and 22 may generate and provide session WEP keys in compliance with the IEEE 802.11 standard. The procedure for generating a handoff WEP key may be the same as that for generating a session WEP key.

[0040] Each access point 14, 16, 18, or 22 may be operable to handoff a terminal to another access point 14, 16, 18, or 22 (handoff access point). During a handoff of a wireless terminal, the handing off access point 14, 16, 18 may provide a handoff WEP key to the wireless terminal. For security reasons, the access points 14, 16, 18, and 22 may deliver a handoff WEP key only to wireless terminals that are "actively" communicating at the time of a handoff. Actively communicating may include running a real-time application, such as a streaming video application or a VoIP application, downloading a file, or otherwise sending or receiving packets. If a terminal is merely associated with an access point 14, 16, 18, or 22 at the time of a handoff, then a handoff WEP key may not provide to the terminal.

[0041] During a handoff of a terminal to one of the access points 14, 16, 18, or 22, the access point and the terminal may exchange handoff authentication messages. An illustrative handoff authentication message exchange is shown in Table 1.

TABLE 1

Wireless Terminal	Handoff Access Point
• Terminal Identity Assertion • Auth. Algorithm ID = "handoff WEP" • Auth. transaction sequence number = 1 • Auth. algorithm dependent information = (none)	
	• Auth. Algorithm ID = "handoff WEP" • Auth. transaction sequence number = 2 • Auth. algorithm dependent information = challenge text. • Result of the requested authentication
• Auth. Algorithm ID = "handoff WEP" • Auth. transaction sequence number = 3 • Auth. algorithm dependent information = challenge text encrypted by handoff WEP key	
	• Auth. Algorithm ID= "handoff WEP" • Auth. transaction sequence number = 4 • Auth. algorithm dependent information = the authentication result

[0042] Each handoff authentication message may include an authentication algorithm number to indicate an authentication algorithm for processing the message. For example, "2" may indicate a handoff WEP key algorithm, "1" may indicated a shared key (session key) algorithm, and "0" may indicate an open system (null authentication) algorithm. For the handoff WEP key algorithm, a handoff WEP key may be used to encrypt and decrypt challenge text.

[0043] FIG. 3 shows a shared key handoff authentication procedure using a handoff WEP key. The access points 14 and 16 are both associated with the AAAF server 32. Therefore, access points 14 and 16 may receive a common handoff WEP key from the AAAF server 32 at 302. The handoff WEP key transmission may be encrypted by an encryption key shared by the AAAF server 32 and the access points 14 and 16. At 304, the wireless terminal 12 is in association with and communicating through the access point 14. Communication between the wireless terminal 12 and the access point 14 may be encrypted by a session WEP key.

[0044] To facilitate a quick handoff, the wireless terminal 12 may request a handoff WEP key at 306. The access point 14 may deliver the handoff WEP key to the wireless terminal 12 at 308. The access point 14 may deliver the handoff WEP key securely by encrypting it with the session WEP key. Rather than transmitting the actual handoff WEP

key, the access point 14 may deliver a seed to generate the handoff WEP key.

[0045] The wireless terminal 12 may decide to handoff from the access point 14 to the access point 16 (handoff access point) at handoff decision 310. To begin the handoff, the wireless terminal 12 may exchange probe request and response packets with the handoff access point 16 at 312. If the probe is successful, then at 314 the wireless terminal 12 may exchange handoff authentication messages with the handoff access point 16. The handoff authentication message exchange at 314 may transpire as described above in Table 1.

[0046] If the handoff authentication is successful, then at 316 the wireless terminal 12 may exchange association request and response packets with the handoff access point 16. If successful, then at 316 the wireless terminal 12 may be associated with the handoff access point 16. After the wireless terminal 12 and the handoff access point 16 are associated, data communicated between them at 318 may be encrypted with the handoff WEP. The wireless terminal 12 and the handoff access point 16 may continue to communicate data encrypted by the handoff WEP key until the handoff access point 16 provides a new session WEP key at 326.

[0047] For example, the wireless terminal 12 may require a new mobile internet protocol (IP) address in order to communicate via the Internet after association with the handoff access point 16. The handoff WEP key may be used at 318 to encrypt packets relating to mobile IP address acquisition. Illustratively, the wireless terminal 12 may communicate with a dynamic host control protocol (DHCP) server (not shown) at 318 in order to request and receive a new mobile IP address. The wireless terminal 12 may also send a binding update message at 318 that indicates the new mobile IP address. The handoff WEP key may provide sufficient security for packets relating to mobile IP address acquisition.

[0048] For a further example, the wireless terminal 12 may be running a running a real-time application at the time of the handoff. At 318, data packets sent and received by the real-time application may be encrypted by the handoff WEP key for communication via the handoff access point 16. Thus, the real-time application of the wireless terminal 12 may continue communicating with no perceivable interruption during the handoff.

[0049] At 320, the wireless terminal 12 may communicate terminal authentication packets to the handoff access point 16. The terminal authentication packets may be encrypted by the handoff WEP key. However, it may not be necessary to encrypt the terminal authentication packets.

[0050] At 322, the handoff access point 16 may communicate the terminal authentication packets to the AAAH server 36. After the AAAH server 36 verifies the identity or credentials of the wireless terminal 12, at 324 the AAAH server 36 may communicate terminal authorization packets to the handoff access point 16. The handoff access point 16 may provide a new session WEP key may to the wireless terminal 12 at 326.

[0051] At 328, the wireless terminal 12 and the handoff access point 16 may switch from using the handoff WEP key to using the new session WEP key for encryption. The new session WEP key may be used to encrypt communications between the wireless terminal 12 and the handoff access point 16 until another handoff occurs, or communications cease for some other reason.

[0052] The shared key handoff authentication procedure described above may also be used for a handoff of the wireless terminal 12 from access point 16 to access point 18. With a one additional action, this procedure may further be used for a handoff of the wireless terminal 12 from access point 18 to access point 22. In this one additional action, the AAAH server 36 may generate and provide the handoff WEP key to the AAAF severs 32 and 34, or directly to the access points 14, 16, 18 and 22. This action provides a common handoff WEP key to access points 18 and 22.

[0053] Other methods of generating and communicating a handoff WEP key may be implemented without departing from the scope of the claimed invention. For example, the AAAF sever 32 may generate the handoff WEP key, and communicate it to the AAAH server 36. The AAAH server 36 may then communicate the handoff WEP key to the AAAF sever 34. The methods described herein are merely illustrative.

[0054] The shared key handoff authentication procedure shown in FIG. 3 may require a firmware modification for use by some existing equipment. Therefore, an open system handoff authentication procedure is provided in FIG. 4. The open system handoff authentication procedure may comply with the IEEE 802.11 standard, and further with the IEEE 802.1x standard.

[0055] Many items of the open system handoff authentication procedure may operate in essentially the same manner as items in the shared key handoff authentication procedure. Items 402, 404, 406, 408, 410, and 412 of the open system handoff authentication procedure may operate in the same manner as items 302, 304, 306, 308, 310, and 312 in the shared key handoff authentication procedure, respectively. At 414, however, the handoff authentication message exchange may use an "open system" authentication algorithm rather than the "handoff WEP key" authentication algorithm used at 312.

[0056] Using the open system authentication algorithm, the handoff access point 16 may authenticate the wireless terminal 12 for handoff without a challenge (a null authentication). After this null authentication, at 416 the wireless terminal 12 may associate with the handoff access point 16. Data packets communicated between the wireless terminal 12 and the handoff access point 16 at 418 may be encrypted by the handoff WEP key.

[0057] At step 420, the wireless terminal 12 may communicate terminal authentication packets to the handoff access

point 16. Like in 420 above, the terminal authentication packets may be encrypted by the handoff WEP key at 420. Again, however, encryption of the terminal authentication packets may not be necessary. At 422, 424, 426, and 428, the open system handoff authentication procedure may operate in essentially the same manner the shared key handoff authentication procedure at 322, 324, 326, and 328, respectively

[0058] The open system authentication procedure may not challenge the wireless terminal 12 at 414. Therefore, the handoff access point 16 may include a security procedure that allows the wireless terminal 12 to communicate unencrypted terminal authentication packets to the AAAH server 36. Furthermore, the security procedure may allow the wireless terminal 12 to communicate data packets to the network 8 only if the data packets are encrypted with the handoff WEP key. Illustrative security procedures are shown in FIGS. 5 and 6.

[0059] FIG. 5 shows one security procedure for the handoff access point 16. The security procedure may operate at a data link layer of the handoff access point 16. The security procedure may delete unauthorized packets, while transferring packets from verified media access control (MAC) addresses, terminal authentication packets, and handoff WEP encrypted packets to a higher network layer. When a packet is transferred to a higher network layer, it may continue on towards a destination node.

[0060] The handoff access point 16 may register MAC addresses of wireless terminals that are verified and have an associated session WEP key. The handoff access point 16 may receive a packet from the wireless terminal 12. At 502, the handoff access point 16 may determine from origination MAC address of the packet whether the wireless terminal 12 is verified. If so, then the handoff access point 16 will have a session WEP key for the wireless terminal 12. The session WEP key may be used to decrypt the received packet at 504. The decrypted packet may then be transferred to a higher network layer at 516.

[0061] On the other hand, if the wireless terminal 12 is not verified, then at 506 and 510 the packet may be further analyzed. At 506, the handoff access point 16 may determine whether the packet is an unencrypted terminal authentication packet destined for the AAAH 36. If so, then packet may then be transferred to a higher network layer at 516. If not, then the packet may be deleted at 508.

[0062] At 510, the handoff access point 16 may determine whether the packet is encrypted by the handoff WEP key. If so, then packet may be decrypted at 514. The decrypted packet may then be transferred to a higher network layer at 516. If the packet is not encrypted by the handoff WEP key, then the packet may be deleted at 512.

[0063] By operation of the security procedure, packets encrypted by the handoff WEP key may be transferred to a higher network layer. Likewise, unencrypted terminal authentication packets may be transferred to a higher network layer. All other packets, including unencrypted or improperly encrypted data packets, may be deleted.

[0064] FIG. 6 shows another security procedure for the handoff access point 16. There is one main difference between the security procedure shown in FIG. 6 and the one shown in FIG. 5. In the security procedure shown in FIG. 6, the received packet is processed in serial rather than in parallel. Items 602 and 604 operate essentially the same as items 502 and 504, respectively. If the MAC address has not been verified, then the handoff access point 16 may proceed from 602 to 606.

[0065] At step 606, the handoff access point 16 may determine whether the packet is an unencrypted terminal authentication packet bound for the AAAH 36. If so, then the packet may be transferred to a higher network layer at 614. If not, at 608 the handoff access point 16 may determine whether the packet is encrypted by the handoff WEP key.

[0066] If the packet is encrypted by the handoff WEP key, then at 612 the packet may be decrypted. The decrypted packet may be transferred to a higher network layer at 614. If the packet is not encrypted by the handoff WEP key, then at 610 the packet may be deleted. As with the security procedure of FIG. 5, packets encrypted by the handoff WEP key and unencrypted terminal authentication packets may be transferred to a higher network layer, while all other packets may be deleted.

[0067] The open system handoff authentication procedure shown in FIG. 4 may implement the security procedure shown in FIG. 5 or the security procedure shown in FIG. 6. In either case, the open system handoff authentication procedure may operate with a wireless terminal 12 that does not support a handoff WEP key authentication algorithm.

[0068] For example, even though such a wireless terminal 12 may not accept a handoff WEP key at 408, it may still probe, be handoff authenticated by, and be associated with the handoff access point 16 at 410, 412, and 414. At 416, the wireless terminal 12 may not communicate data packets because it has no handoff WEP key with which to encrypt them. Any unencrypted data packets the wireless terminal 12 sends to the handoff access point 16 may be deleted by operation of the security procedures shown in FIG. 5 or FIG. 6.

[0069] Unencrypted terminal authentication packets from the wireless terminal 12, however, may still be communicated to the AAAH server 36. Therefore, the AAAH server 36 may still authenticate and authorize the wireless terminal 12. Consequently, the handoff access point 16 may still provide the wireless terminal 12 with a new session WEP key at 424, thereby allowing for encrypted data communications at step 426.

[0070] While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. Accordingly, the invention is not to be restricted except in light of the attached claims and their equivalents.

Claims

1. A method for handover in a wireless communication network, comprising the steps of:

   providing a handoff WEP key to a first access point and a second access point;
   transmitting the handoff WEP key from the first access point to a wireless terminal associated with the first access point;
   authenticating the wireless terminal with the second access point; and
   communicating data packets encrypted with the handoff WEP key between the second access point and the wireless terminal.

2. The method of claim 1, where transmitting the handoff WEP key from the first access point to the wireless terminal further includes the step of encrypting the handoff WEP key with a session WEP key.

3. The method of claim 1, further including the step of authenticating the wireless terminal with an authentication server.

4. The method of claim 3, where authenticating the wireless terminal with the authentication server further includes communicating terminal authentication packets via the second access point between the wireless terminal and the authentication server.

5. The method of claim 4, where communicating terminal authentication packets includes encrypting the terminal authentication packets with the handoff WEP key.

6. The method of claim 4, where communicating the terminal authentication packets includes transmitting the terminal packets unencrypted.

7. The method of claim 3, where authenticating the wireless terminal with the second access point further includes transmitting terminal authorization packets from the authentication server to the second access point.

8. The method of claim 3, further including the step of transmitting a session WEP key from the second access point to the wireless terminal after the wireless terminal is authenticated by the authentication server.

9. The method of claim 1, where providing the handoff WEP key further includes generating the handoff WEP key with a server, and transmitting the handoff WEP key from the server to the first access point and the second access point.

10. The method of claim 1, where authenticating the wireless terminal further includes sending a challenge message encrypted with the handoff WEP key from the second access point to the wireless terminal, decrypting the challenge message at the wireless terminal with the handoff WEP key, and transmitting the decrypted challenge message from the wireless terminal to the second access point.

11. The method of claim 1, where transmitting the handoff WEP key from the first access point to the wireless terminal further includes transmitting the handoff WEP key to the wireless terminal if the wireless terminal is actively communicating via the first access point.

12. The method of claim 1, where providing the handoff WEP key further includes generating the handoff WEP key with a server periodically, and transmitting the handoff WEP key from the server to the first access point and the second access point periodically.

13. The method of claim 1, where transmitting the handoff WEP key further includes transmitting a handoff WEP key request from the wireless terminal to the first access point, and transmitting the handoff WEP from the first access point to the wireless terminal in response to the request.

14. The method of claim 1, where transmitting the handoff WEP key further includes transmitting a seed to generate a handoff WEP key from the first access point to the wireless terminal.

15. A wireless network comprising:

a wireless terminal operable to receive a handoff WEP key, encrypt data with the handoffWEP key, and transmit the encrypted data;
a first access point operable to transmit the handoff WEP key to the wireless terminal; and
a second access point operable to receive the encrypted data from the wireless terminal, and decrypt the encrypted data with the handoff WEP key.

16. The wireless network of claim 15, further including a server coupled to the first access point and the second access point, the server operable to generate the handoff WEP key and transmit the handoff WEP key to the first access point and the second access point.

17. The wireless network of claim 15, further including a server coupled to the first access point and the second access point, the server operable to communicate terminal authentication packets with the wireless terminal, authenticate the wireless terminal, and communicate terminal authorization packets with the second access point.

18. A wireless access point having a memory including:

instructions to receive a packet;
instructions to delete the packet if the packet is a data packet that is not encrypted with a handoff WEP key;
instructions to decrypt and transmit the packet if the packet is a data packet that is encrypted with a handoff WEP key; and
instructions to transmit the packet if the packet is a terminal authentication packet.

19. The wireless access point of claim 18, where the memory further includes instructions to read the media access control address of a terminal that sent the packet from the packet, instructions to determine whether the memory includes a session WEP key for the terminal, and instructions to decrypt and transmit the packet where the memory includes a session WEP key for the terminal.

20. A wireless terminal having a memory that includes:

a code segment that receives and decrypts a handoff WEP key that is encrypted with a first session WEP key;
a code segment that encrypts data with the handoff WEP key;
a code segment that transmits the encrypted data; and
a code segment that receives and decrypts a second session WEP key that is encrypted with the handoff WEP key.

21. The wireless terminal of claim 20, where the memory includes a code segment that that encrypts and decrypts data with the first session WEP key until the handoff WEP key is received, a code segment that encrypts and decrypts data with the handoff WEP key until the second session WEP key is received, and a code segment that encrypts and decrypts data with the second session WEP key after the second session WEP is received.

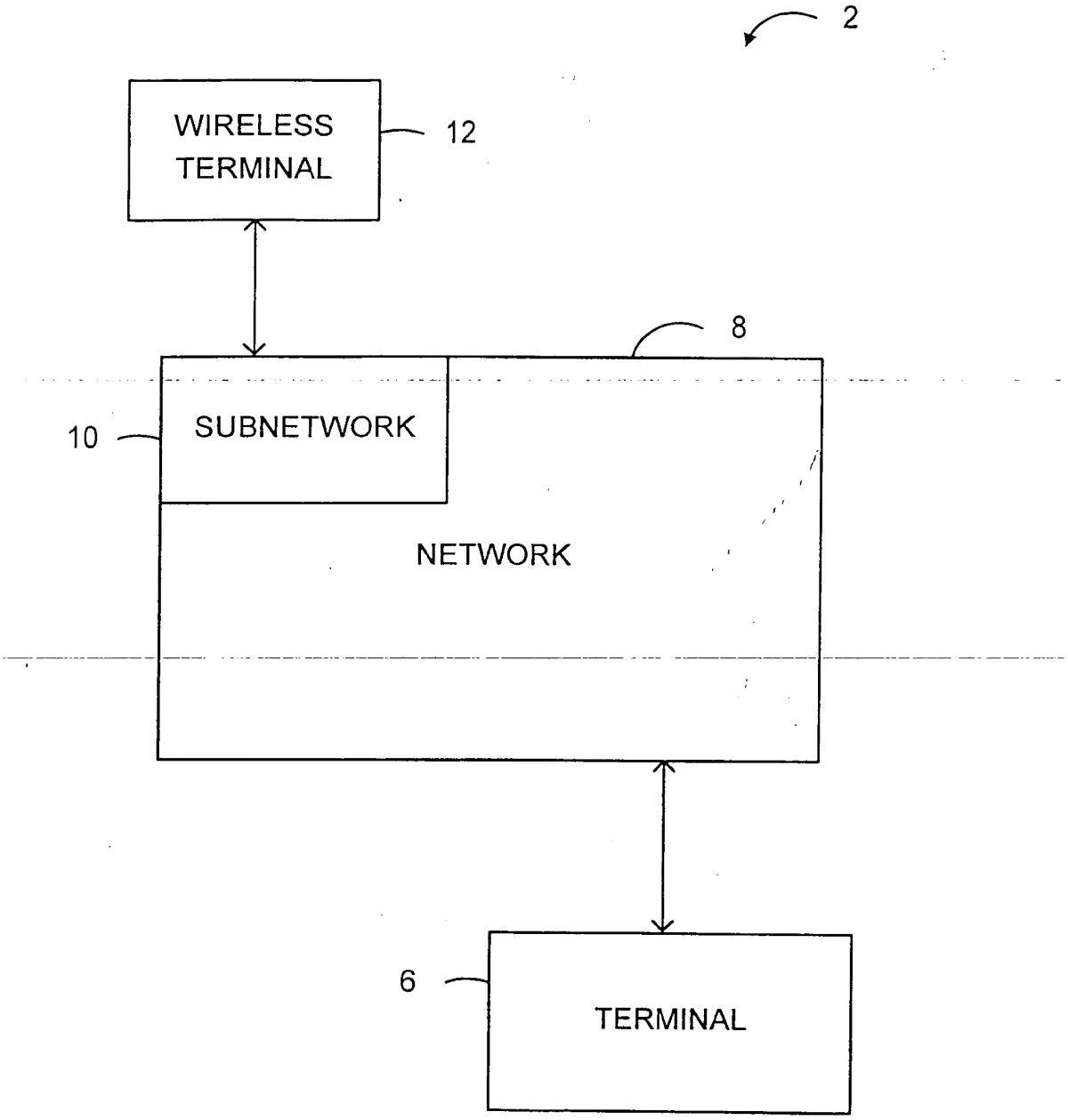


Fig. 1

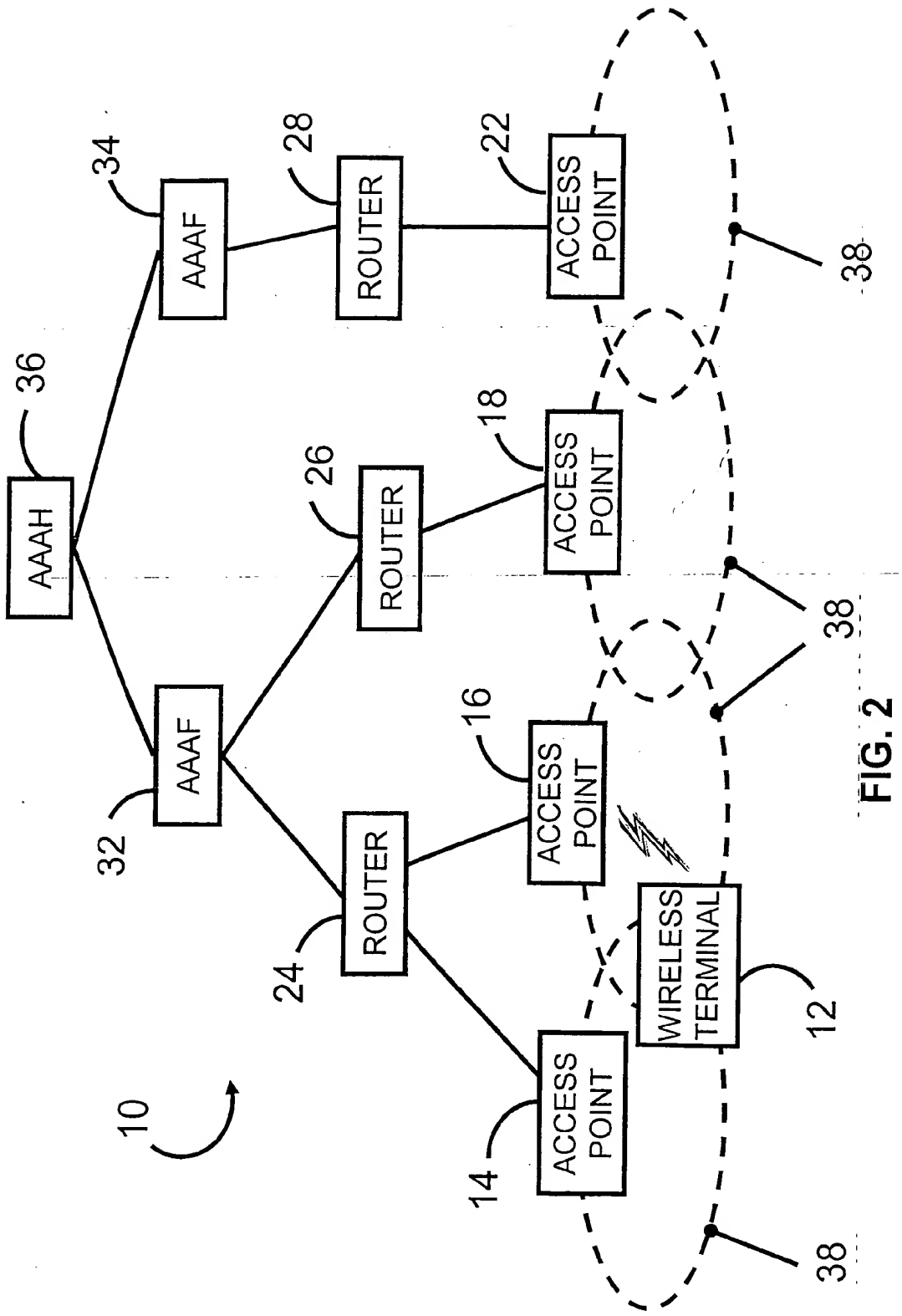
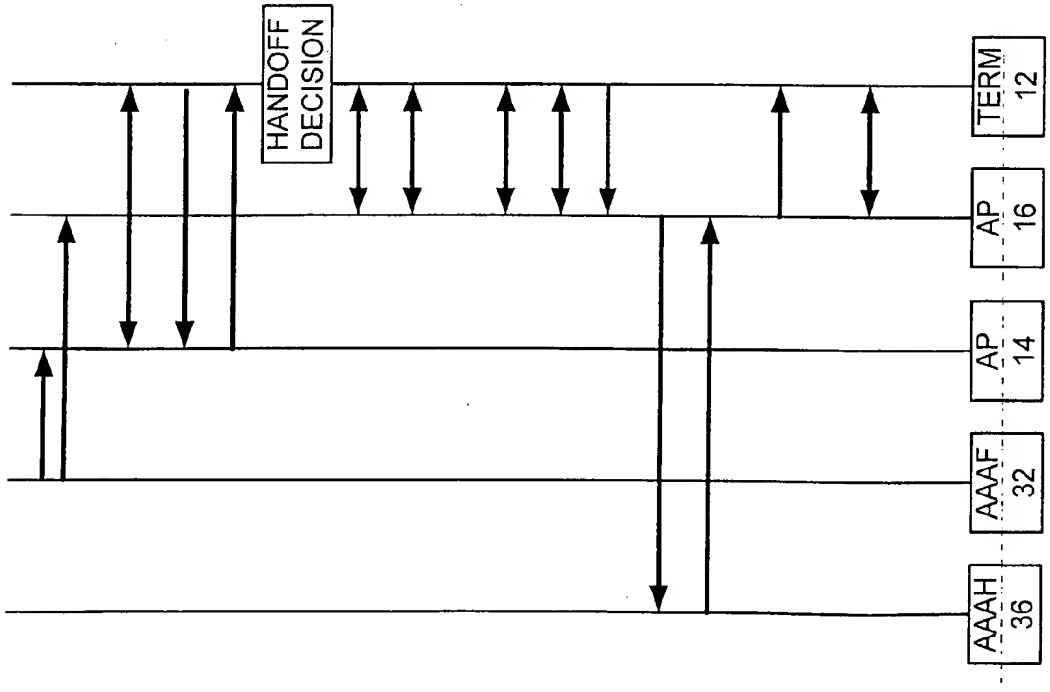

AAAH
AAAF
AAAF
ROUTER
ROUTER
ROUTER
ACCESS POINT
ACCESS POINT
ACCESS POINT
ACCESS POINT
WIRELESS TERMINAL
10
12
14
16
18
22
24
26
28
32
34
36
38
38
38

FIG. 2



302 HO WEP KEY (ENCRYPTED)

304 COMMUNICATIONS (SESSION WEP ENCRYPTED)

306 HO WEP REQUEST (SESSION WEP ENCRYPTED)

308 HO WEP KEY (SESSION WEP ENCRYPTED)

310 HANDOFF DECISION

312 PROBE REQ. & RESP.

314 HANDOFF AUTHENTICATION MESSAGES (HO WEP AUTHENTICATION ALGORITHM)

316 ASSOCIATION REQ. & RESP.

318 COMMUNICATIONS (HO WEP ENCRYPTED)

320 TERM AUTHENTICATION PACKETS (UNENCRYPTED)

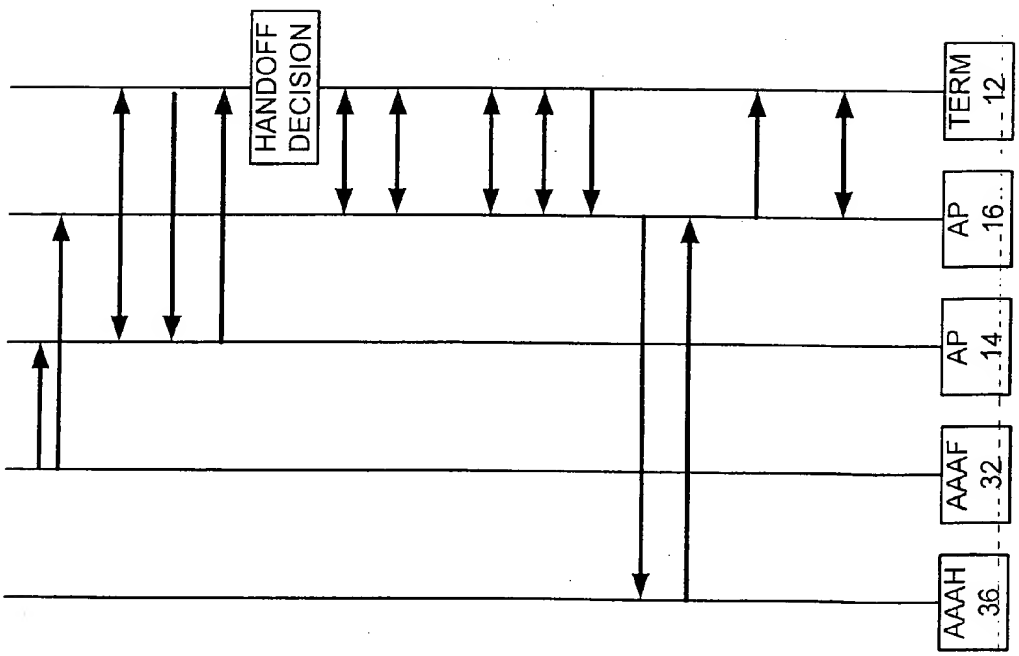
322 TERM AUTHENTICATION PACKETS

324 TERM AUTHORIZATION PACKETS

326 NEW SESSION WEP KEY

328 COMMUNICATIONS (NEW SESSION WEP ENCRYPTED)

FIG. 3



402 HO WEP KEY (ENCRYPTED)

404 COMMUNICATIONS (SESSION WEP ENCRYPTED)

406 HO WEP REQUEST (SESSION WEP ENCRYPTED)

408 HO WEP KEY (SESSION WEP ENCRYPTED)

406 HANDOFF DECISION

410 PROBE REQ. & RESP.

412 HANDOFF AUTHENTICATION MESSAGES (NO TERMINAL VERIFICATION)

414 ASSOCIATION REQ. & RESP.

416 COMMUNICATIONS (HO WEP ENCRYPTED)

418 TERM AUTHENTICATION PACKETS (UNENCRYPTED)

420 TERM AUTHENTICATION PACKETS

422 TERM AUTHORIZATION PACKETS

424 NEW SESSION WEP KEY

426 COMMUNICATIONS (NEW SESSION WEP ENCRYPTED)

FIG. 4

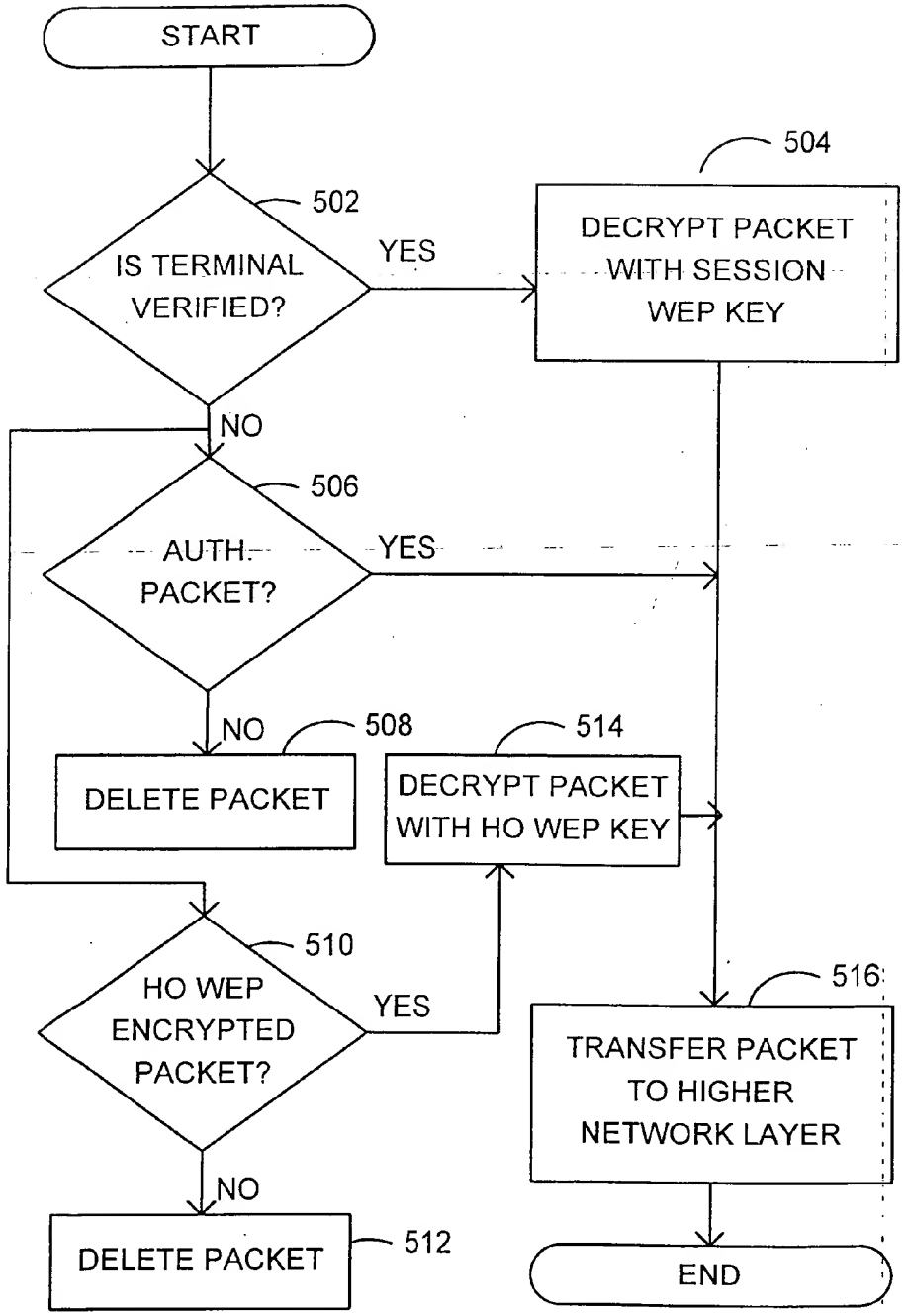

START
502
IS TERMINAL VERIFIED?
YES
504
DECRYPT PACKET WITH SESSION WEP KEY
NO
506
AUTH. PACKET?
YES
NO
508
DELETE PACKET
514
DECRYPT PACKET WITH HO WEP KEY
510
HO WEP ENCRYPTED PACKET?
YES
516
TRANSFER PACKET TO HIGHER NETWORK LAYER
NO
DELETE PACKET
512
END

Fig. 5

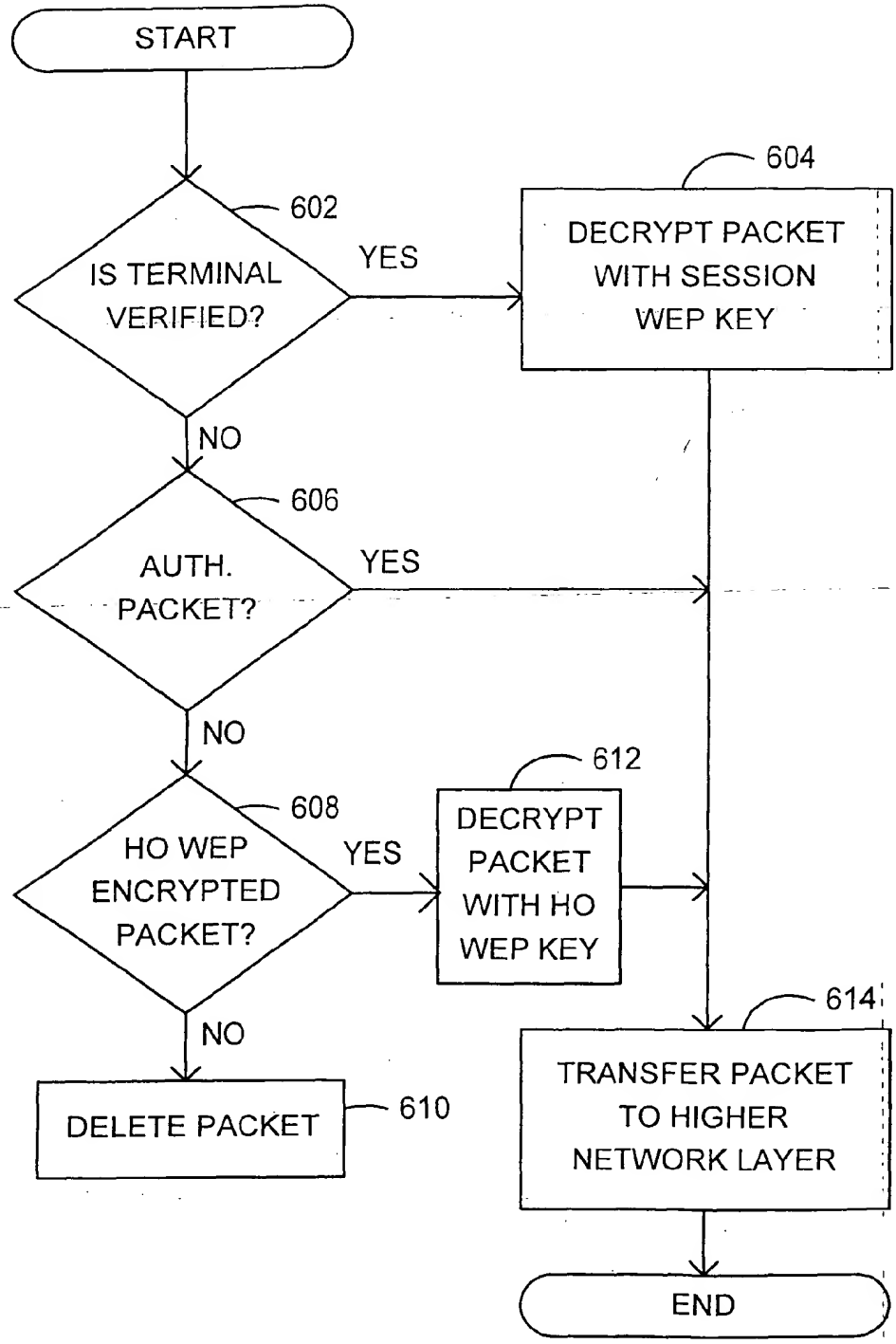

START
602
IS TERMINAL VERIFIED?
YES
604
DECRYPT PACKET WITH SESSION WEP KEY
NO
606
AUTH. PACKET?
YES
NO
608
HO WEP ENCRYPTED PACKET?
YES
612
DECRYPT PACKET WITH HO WEP KEY
NO
DELETE PACKET
610
614
TRANSFER PACKET TO HIGHER NETWORK LAYER
END

Fig. 6

PUB-NO: EP001422875A2
DOCUMENT-IDENTIFIER: EP 1422875 A2
TITLE: Wireless network handoff key
PUBN-DATE: May 26, 2004

INVENTOR-INFORMATION:

NAME	COUNTRY
WU, GANG	US
WATANABE, FUJIO	US
HAGEN, ALEXANDER	US

ASSIGNEE-INFORMATION:

NAME	COUNTRY
DOCOMO COMM LAB USA INC	US

APPL-NO: EP03025633
APPL-DATE: November 6, 2003

PRIORITY-DATA: US29065002A (November 8, 2002)

INT-CL (IPC): H04L012/28

EUR-CL (EPC): H04L012/28 , H04L012/56 , H04L029/06 , H04L029/06 , H04Q007/38

ABSTRACT:

CHG DATE=20060818 STATUS=C>A handoff key is provided for facilitating a handoff of a wireless terminal (12) from a first access point to

a second access point. The handoff key may be generated by a server and communicated to the first and second access points. Alternatively, the handoff key may be generated one of the access points and transmitted to the other access point. The first access point may transmit the handoff key to the wireless terminal before the handoff. Shortly after the handoff, the wireless terminal and the second access point may communicate data encrypted with the handoff key. Later, an authentication server (36) may authenticate the wireless terminal, causing the second access point to provide the wireless terminal (12) with a session key. Thereafter, the wireless terminal (12) and the second access point may communicate data encrypted with the session key.